


Also published as:

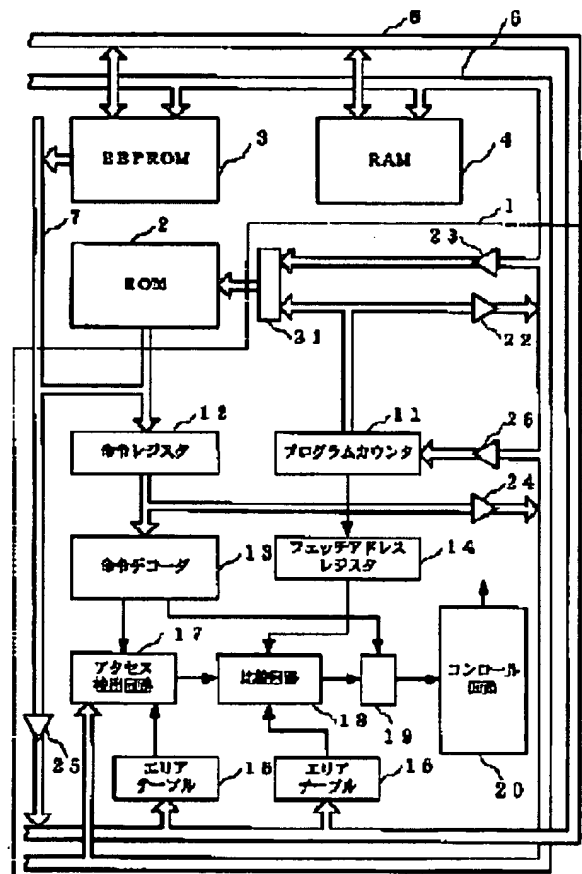
 EP0859319 (A1)

US6101586 (A1)

 CN1145885C (C)

Priority number(s): JP19970030385 19970214

1



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-228421

(43) 公開日 平成10年(1998) 8月25日

(51) Int.Cl.⁸

G 0 6 F 12/14

識別記号

3 2 0

3 1 0

F I

G 0 6 F 12/14

3 2 0 A

3 1 0 H

審査請求 有 請求項の数 2 O L (全 10 頁)

(21) 出願番号

特願平9-30385

(22) 出願日

平成 9 年 (1997) 2 月 14 日

(71) 出願人 000232036

日本電気アイシーマイコンシステム株式会
社

神奈川県川崎市中原区小杉町 1 丁目 403 番
53

(72) 発明者 石本 淳一

神奈川県川崎市中原区小杉町 1 丁目 403 番
53 日本電気アイシーマイコンシステム株
式会社内

(72) 発明者 田中 正則

神奈川県川崎市中原区小杉町 1 丁目 403 番
53 日本電気アイシーマイコンシステム株
式会社内

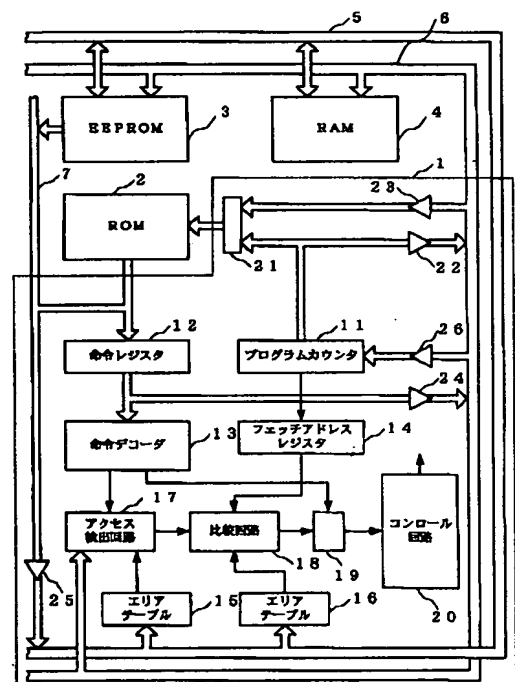
(74) 代理人 弁理士 山川 政樹

(54) 【発明の名称】 メモリアクセス制御回路

(57) 【要約】

【課題】 不正アクセスに対して高い保護機能が得られ
るメモリアクセス制御回路を提供する。

【解決手段】 レジスタ 1 4 はプログラムカウンタ 1 1
の値を保持する。テーブル 1 5 はメモリ上の保護領域の
アドレスを保持し、テーブル 1 6 は保護領域へのアクセ
スが許されている命令のアドレスを保持する。アクセス
検出回路 1 7 は、命令の解釈結果、アクセス先のアドレ
スとテーブル 1 5 のアドレスの比較結果に基づき、保護
領域へのアクセス命令かどうかを判定する。比較回路 1
8 は、保護領域へのアクセス命令が検出されたとき、レ
ジスタ 1 4、テーブル 1 6 のアドレスを比較して、保護
領域へのアクセスが許されていないエリアから読み出さ
れた命令と判断したときに禁止信号を出力して、不正な
メモリアクセスを禁止する。



【特許請求の範囲】

【請求項１】 メモリ上の保護すべき領域に対するアクセスを検出して不正なアクセスを禁止するメモリアクセス制御回路であって、
実行すべき命令が格納されたメモリ上の位置を表す命令フェッチアドレスを保持する第１のアドレス保持手段と、
前記保護領域のアドレスを保持する第２のアドレス保持手段と、
前記保護領域へのアクセスが許されている命令のメモリ上の位置を表す命令フェッチアドレスを保持する第３のアドレス保持手段と、
メモリから読み出された命令の解釈結果、及びこの命令が示すアクセス先のアドレスと第２のアドレス保持手段に保持されたアドレスの比較結果に基づいて、保護領域へのアクセス命令かどうかを判定するアクセス検出手段と、
このアクセス検出手段により保護領域へのアクセス命令が検出されたとき、第１、第３のアドレス保持手段に保持された命令フェッチアドレスを比較して、保護領域へのアクセスが許されていない格納位置から読み出された命令と判断したときに禁止信号を出力する比較手段と、
禁止信号が出力されたときにメモリアクセスを禁止する禁止手段とを有することを特徴とするメモリアクセス制御回路。

【請求項２】 メモリ上の保護すべき領域に対するアクセスを検出して不正なアクセスを禁止するメモリアクセス制御回路であって、
実行すべき命令が格納されたメモリ上の位置を表す命令フェッチアドレスを保持する第１のアドレス保持手段と、
前記保護領域のアドレスを保持する第２のアドレス保持手段と、
前記保護領域への分岐が許されている分岐命令のメモリ上の位置を表す命令フェッチアドレスを保持する第３のアドレス保持手段と、
メモリから読み出された命令の解釈結果、及びこの命令が示す分岐先のアドレスと第２のアドレス保持手段に保持されたアドレスの比較結果に基づいて、保護領域への分岐命令かどうかを判定するアクセス検出手段と、
このアクセス検出手段により保護領域への分岐命令が検出されたとき、第１、第３のアドレス保持手段に保持された命令フェッチアドレスを比較して、保護領域への分岐が許されていない格納位置から読み出された命令と判断したときに禁止信号を出力する比較手段と、
禁止信号が出力されたときに分岐命令の実行を禁止する禁止手段とを有することを特徴とするメモリアクセス制御回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータシステム等におけるメモリアクセス制御回路に係り、特にメモリ上の保護すべき領域に対するアクセスを検出して不正なアクセスを禁止するメモリアクセス制御回路に関するものである。

【０００２】

【従来の技術】従来より、コンピュータプログラムの開発は多大な時間を要する作業である。コンピュータプログラムの開発者は、そのプログラムを売ることによって開発費用を賄ってきた。しかし、第３者がメモリ上のプログラムやデータを読み出すためのプログラムを作成して、メモリからプログラムやデータを読み出すことは可能であり、このようなコピーが容易に行われると、開発費用を賄うことは困難となる。また、暗号アルゴリズムに用いる暗号処理ルーチンやデータがメモリに書き込まれている暗号回路において、これらのデータがメモリから読み出されてしまうと、暗号化する前の平文が解読されてしまうことになる。

【０００３】そこで、このようなメモリへの不正アクセスを防止するためのメモリアクセス制御回路が提案されている（例えば、特開昭５９－１１６００号公報）。図６は特開昭５９－１１６００号公報に開示された従来のメモリアクセス制御回路のブロック図である。このメモリアクセス制御回路は、ＣＰＵ３１、不揮発性メモリ３２、一時的メモリ３３、外部インタフェース手段３４、アドレスバス３５、データバス３６、不揮発性メモリ３２に記憶された情報の保護状況を示すプログラム保護ビット３７、不揮発性メモリ３２へのアクセスを判断するアドレス論理３８、外部インタフェース手段３４の操作を禁止するための外部インタフェース禁止論理手段３９、不揮発性メモリ３２の操作を禁止するための操作禁止バッファ４０、一時的メモリ３３の操作を禁止するための操作禁止バッファ４１、命令の取得がいつ行われるかを判断する命令取得論理４２から構成されている。

【０００４】このような構成により、このメモリアクセス制御回路は、不揮発性メモリ３２又は一時的メモリ３３の保護すべき領域から保護されていない領域への情報の転送を禁止する。こうして、第３者が一時的メモリ３３上のプログラムを実行することで、不揮発性メモリ３２上の保護すべきデータを一時的メモリ３３上に不正に読み出すことができなくなる。

【０００５】

【発明が解決しようとする課題】しかし、このような従来のメモリアクセス制御回路では、メモリ間のデータ転送を禁止しているだけなので、メモリ上の保護すべきデータをＣＰＵのアクキュレータ等の汎用レジスタに一旦読み出して、これに何らかの演算を加えた後にメモリに読み出すことは禁止できず、このような演算結果を得ることで保護すべき元のデータが判明してしまうという問題点があった。例えば、保護領域内のデータをアクキュ

レータに読み出し、これに「0」を加算するといった簡単な演算をした後に、演算結果をメモリに読み出せば、保護すべき元のデータを容易に知ることができる。また、ある演算を行ったときのCPUが内蔵するステータスフラグ（例えばキャリフラグなど）の状態変化を調べることで、保護すべき元データを間接的に知ることができる。本発明は、上記課題を解決するためになされたもので、不正アクセスに対して高い保護機能が得られるメモリアクセス制御回路を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明のメモリアクセス制御回路は、請求項1に記載のように、実行すべき命令が格納されたメモリ上の位置を表す命令フェッチアドレスを保持する第1のアドレス保持手段と、メモリ上の保護すべき領域のアドレスを保持する第2のアドレス保持手段と、保護領域へのアクセスが許されている命令のメモリ上の位置を表す命令フェッチアドレスを保持する第3のアドレス保持手段と、メモリから読み出された命令の解読結果、及びこの命令が示すアクセス先のアドレスと第2のアドレス保持手段に保持されたアドレスの比較結果に基づいて、保護領域へのアクセス命令かどうかを判定するアクセス検出手段と、このアクセス検出手段により保護領域へのアクセス命令が検出されたとき、第1、第3のアドレス保持手段に保持された命令フェッチアドレスを比較して、保護領域へのアクセスが許されていない格納位置から読み出された命令と判断したときに禁止信号を出力する比較手段と、禁止信号が出力されたときにメモリアクセスを禁止する禁止手段とを有するものである。このように、アクセス検出手段によって保護領域へのアクセス命令かどうかを判定し、保護領域へのアクセス命令が検出されたとき、保護領域へのアクセスが許されている格納位置から読み出された命令かどうかを比較手段によって判断して、保護領域へのアクセスが許されていない格納位置から読み出された命令と判断したときに禁止信号を出力し、禁止手段によってメモリアクセスを禁止することにより、保護領域への不正なアクセスを禁止することができる。

【0007】また、請求項2に記載のように、実行すべき命令が格納されたメモリ上の位置を表す命令フェッチアドレスを保持する第1のアドレス保持手段と、保護領域のアドレスを保持する第2のアドレス保持手段と、保護領域への分岐が許されている分岐命令のメモリ上の位置を表す命令フェッチアドレスを保持する第3のアドレス保持手段と、メモリから読み出された命令の解読結果、及びこの命令が示す分岐先のアドレスと第2のアドレス保持手段に保持されたアドレスの比較結果に基づいて、保護領域への分岐命令かどうかを判定するアクセス検出手段と、このアクセス検出手段により保護領域への分岐命令が検出されたとき、第1、第3のアドレス保持手段に保持された命令フェッチアドレスを比較して、保

護領域への分岐が許されていない格納位置から読み出された命令と判断したときに禁止信号を出力する比較手段と、禁止信号が出力されたときに分岐命令の実行を禁止する禁止手段とを有するものである。このように、アクセス検出手段によって保護領域への分岐命令かどうかを判定し、保護領域への分岐命令が検出されたとき、保護領域への分岐が許されている格納位置から読み出された命令かどうかを比較手段によって判断して、保護領域への分岐が許されていない格納位置から読み出された命令と判断したときに禁止信号を出力し、禁止手段によって分岐命令の実行を禁止することにより、保護領域への不正な分岐を禁止することができる。

【0008】

【発明の実施の形態】

実施の形態の1. 以下、本発明の実施の形態について図面を参照して説明する。図1は本発明の第1の実施の形態を示すメモリアクセス制御回路のブロック図である。本実施の形態のメモリアクセス制御回路は、CPU1、製造時に書き込みが行われ以後は書き換えることのできないマスクROM（Read Only Memory）2、書き込みと消去が電氣的に可能なEEPROM（Electrically Erasable and Programmable ROM）3、RAM（Random Access Memory）4、データ情報をやり取りするためのデータバス5、アドレス情報をやり取りするためのアドレスバス6、インストラクションバス7から構成されている。

【0009】そして、CPU1は、図示しないアキュムレータ等の汎用レジスタや論理演算ユニットの他に、実行すべき命令が格納されたメモリ上の位置を表すプログラムカウンタ11、メモリから取り出された命令語を保持する命令レジスタ12、この命令レジスタ12に格納された命令語を解読する命令デコーダ13、プログラムカウンタ11の出力である命令フェッチアドレスを保持する第1のアドレス保持手段となる命令フェッチアドレスレジスタ14、メモリ上の保護すべき領域のアドレスを保持する第2のアドレス保持手段となるエリアテーブル15、保護領域へのアクセスが許されている命令のメモリ上の位置を表す命令フェッチアドレスを保持する第3のアドレス保持手段となるエリアテーブル16、デコーダ13による命令の解読結果、及びこの命令が示すアクセス先のアドレスとテーブル15に保持されたアドレスの比較結果に基づいて、保護領域へのアクセス命令かどうかを判定するアクセス検出回路17、この検出回路17により保護領域へのアクセス命令が検出されたとき、レジスタ14、テーブル16に保持された命令フェッチアドレスを比較して、保護領域へのアクセスが許されていない格納位置から読み出された命令と判断したときに禁止信号を出力する比較回路18、禁止信号が出力されたときにデコーダ13からコントロール回路20への信号を抑止するゲート回路、セクタ21、バッファ

22～26から構成されている。そして、命令デコーダ13、ゲート回路19、コントロール回路20が禁止手段を構成している。

【0010】本実施の形態のメモリアクセス制御回路は、マスクROM2及びEEPROM3が実行命令を格納するプログラムエリアとデータを格納するデータエリアをそれぞれ有し、マスクROM2あるいはEEPROM3上の保護すべき領域に書き込まれたデータ（例えば、暗号アルゴリズムに用いられる暗号鍵）を保護するためのものである。

【0011】次に、このようなメモリアクセス制御回路の動作を説明する。図2はメモリアクセス制御回路の動作を説明するためのタイミングチャート図である。このメモリアクセス制御回路を含むコンピュータシステムは、プログラムカウンタ11から出力される命令フェッチアドレスに従って、ROM2あるいはROM3から命令語を逐次取り出し、解釈して実行する。

【0012】ROM2あるいはROM3から命令を取り出す命令フェッチ時、命令デコーダ13からの制御信号により、セクタ21はプログラムカウンタ11の出力を選択し、バッファ22はイネーブル状態となっている。これにより、プログラムカウンタ11から出力された命令フェッチアドレスは、セクタ21を介してマスクROM2に与えられ、バッファ22、アドレスバス6を介してEEPROM3に与えられる。

【0013】この命令フェッチアドレスがマスクROM2に割り当てられたアドレスであれば、ROM2の該当アドレスの命令語がインストラクションバス7に出力され、EEPROM3に割り当てられたアドレスであれば、ROM3の該当アドレスの命令語がインストラクションバス7に出力される。そして、インストラクションバス7に出力された命令語は、命令レジスタ12に格納される。

【0014】ところで、命令語は、操作を指定する命令コードと、操作の対象となるデータ（オペランド）を指定するオペランドコードとからなる。今、ROM2あるいはROM3にアクセスする命令語（ここでは、データ読み出し命令とする）が2バイト2ステート（命令コードが1バイト、オペランドコードが1バイト）の命令形式であったとすると、命令フェッチアドレスは、図2

(b)に示すように、前の命令の最終ステートにおいて、データ読み出し命令の命令コードが格納されている位置を指すアドレスADとなり、次のステートにおいて、その命令のオペランドコードが格納されている位置を指すアドレスAD+1となる。

【0015】したがって、命令レジスタ12には、図2(d)に示すように、前の命令サイクルの最終ステートにおいて命令コードが格納され、次のステートにおいてオペランドコードが格納される。一方、図2(c)に示すように、プログラムカウンタ11から出力される命令

フェッチアドレスのうち、命令コードのアドレスADが命令フェッチアドレスレジスタ14に格納される。このレジスタ14は、次の命令フェッチによって内容が更新されるまで、その内容を保持し続ける。

【0016】続いて、命令デコーダ13は、命令レジスタ12に格納された命令コードをこの命令サイクルの最初のステートで解釈し、データ読み出し命令であれば、制御信号を出力して、バッファ23～25をイネーブル状態にし、セクタ21がバッファ23の出力を選択するように制御する。これにより、命令コードの次に命令レジスタ12に格納されるオペランドコードがデータアクセス先のアドレスMとしてバッファ24を介してアドレスバス6に出力され、バッファ23、セクタ21を介してROM2に与えられ、アドレスバス6を介してEEPROM3に与えられる。

【0017】また、命令デコーダ13は、命令コードの解釈結果がデータ読み出し命令であれば、データ読み出し命令であることを示す制御信号を出力する。この信号はゲート回路19を通過してコントロール回路20に入力される。このゲート回路の動作については後述する。これにより、コントロール回路20からメモリリード信号が出力される。

【0018】メモリリード信号が出力されたとき、マスクROM2に与えられたアドレスがROM2に割り当てられたアドレスであれば、ROM2の該当アドレスのデータがバッファ25を介してデータバス5に出力され、EEPROM3に割り当てられたアドレスであれば、ROM3の該当アドレスのデータがデータバス5に出力される。このデータバス5に出力されたデータは、CPU1内の図示しないアキュムレータ等の汎用レジスタに格納される。こうして、データ読み出し命令のフェッチと実行が終了する。

【0019】以上のような命令フェッチと命令実行において、メモリから読み出された命令が保護領域へのアクセス命令であった場合には、その命令がどのメモリエリアから読み出されたものかを識別して、保護領域へのアクセスが許されているエリアから読み出された命令であれば、通常通り命令の実行を継続するが、保護領域へのアクセスが許されていないエリアから読み出された命令であれば、メモリアクセス操作を禁止する。次に、この動作について説明する。

【0020】まず、エリアテーブル15には、マスクROM2あるいはEEPROM3内の保護領域のアドレスが格納され、エリアテーブル16には、保護領域へのアクセスが許されている命令の命令フェッチアドレスが格納されている。これらの情報を設定するには、エリアテーブル15、16にアドレス情報を書き込むためのプログラムをROM2あるいはROM3に格納しておき、立ち上げ時にエリアテーブル15、16に書き込みが行われるようにすればよい。また、エリアテーブル15、1

6をROMとし、プログラムの作成時に書き込みを行うようにしてもよい。

【0021】アクセス検出回路17は、命令デコーダ13がメモリアクセス命令であると識別したとき、エリアテーブル15に保持されたアドレスとアドレスバス6に出力されたアドレス（オペランドコードから得られたデータアクセス先のアドレス）とを比較して、保護領域へのアクセス命令かどうかを判定する。

【0022】ここで、エリアテーブル15に登録されたアドレスは、保護領域のアドレスなので、例えば「8000」番地から「8FFF」番地のように特定のアドレス範囲に登録されている。したがって、アクセス検出回路17は、テーブル15に登録されたアドレス範囲中にアドレスバス6に出力されたアドレスと一致するものがあれば、保護領域へのアクセス命令と判断し、一致するものがなければ、保護領域へのアクセス命令ではないと判断する。

【0023】また、エリアテーブル15に登録されたアドレス範囲中に該当するアドレスがあるかどうかを調べればよいので、アドレスの全ビットを比較しなくてもよい。例えば、テーブル15に登録されたアドレスが「8000」番地から「8FFF」番地であれば、この16ビットのアドレス情報の上位4ビットが「1000」なので、上位4ビットのみ比較すればよい。

【0024】続いて、比較回路18は、アクセス検出回路17が保護領域へのアクセス命令であると判断したとき、命令フェッチアドレスレジスタ14に保持された命令フェッチアドレスとエリアテーブル16に保持された命令フェッチアドレスとを比較して、保護領域へのアクセスが許されているエリアから読み出された命令かどうかを判定する。

【0025】このとき、エリアテーブル16にも特定のアドレス範囲に登録されているので、比較回路18は、エリアテーブル16に登録された命令フェッチアドレス中に命令フェッチアドレスレジスタ14に保持された命令フェッチアドレスと一致するものがあれば、保護領域へのアクセスが許されているエリアから読み出された命令であると判断し、一致するものがなければ、保護領域へのアクセスが許されていないエリアから読み出された命令であると判断する。そして、比較回路18は、保護領域へのアクセスが許されていないエリアから読み出された命令であると判断したときに、禁止信号を出力する。

【0026】ゲート回路19は、比較回路18から禁止信号が出力されると、命令デコーダ13からコントロール回路20への信号出力を抑止する。これにより、データ読み出し命令であることを示す信号がコントロール回路20に入力されないの、図2（f）の破線で示すメモリアドレス信号RDがコントロール回路20から出力されなくなる。

【0027】こうして、上記のようにエリアテーブル15、16にアドレス情報を予め設定しておけば、保護領域へアクセスしない命令、あるいは保護領域へアクセスする命令であっても、保護領域へのアクセスが許されているエリアから読み出された命令であれば、正常に実行され、一方、保護領域へのアクセスが許されていないエリアから読み出された命令であれば、不正な命令プログラムと判断されて、メモリアクセスが禁止される。

【0028】したがって、第3者がEEPROM3上に不正な命令プログラムを書き込み、ROM2あるいはROM3の保護領域からデータを不正に読み出そうとしても、保護領域からデータを読み出すことはできず、保護領域のデータに対して演算を行うこともできない。

【0029】なお、本実施の形態では、データ読み出し命令について説明しているが、その他のメモリアクセス命令についても同様に適用でき、例えば、EEPROM3へのデータ書き込み命令であれば、上記の説明におけるデータアクセス先のアドレスがメモリ上の書き込み位置となり、メモリアドレス信号がメモリアドレス信号となることは言うまでもない。

【0030】実施の形態の2。図3は本発明の他の実施の形態を示すメモリアクセス制御回路のブロック図であり、図1と同一の構成には同一の符号を付してある。本実施の形態のメモリアクセス制御回路は、マスクROM2あるいはEEPROM3上に例えば暗号処理ルーチンのような第3者に知られたくない命令処理サブプログラムが書き込まれているときに、その処理ルーチン内で行っている処理内容を保護するためのものである。

【0031】このようなメモリアクセス制御回路の動作を説明する。図4、図5はメモリアクセス制御回路の動作を説明するためのタイミングチャート図である。なお、図4は、分岐命令が保護領域への分岐が許されているエリアから読み出された命令であった場合を示し、図5は、分岐命令が保護領域への分岐が許されていないエリアから読み出された命令であった場合を示している。

【0032】ROM2あるいはROM3から命令を取り出す命令フェッチ時、プログラムカウンタ11から出力された命令フェッチアドレスは、実施の形態の1と同様に、セレクタ21を介してマスクROM2に与えられ、パッファ22、アドレスバス6を介してEEPROM3に与えられる。

【0033】この命令フェッチアドレスがマスクROM2に割り当てられたアドレスであれば、ROM2の該当アドレスの命令語がインストラクションバス7に出力され、EEPROM3に割り当てられたアドレスであれば、ROM3の該当アドレスの命令語がインストラクションバス7に出力される。そして、インストラクションバス7に出力された命令語は、命令レジスタ12に格納される。

【0034】今、サブルーチンに分岐する分岐命令が2

バイト2ステートの命令形式であったとすると、命令フェッチアドレスは、図4（b）に示すように、前の命令の最終ステートにおいて、分岐命令の命令コードが格納されている位置を指すアドレスADとなり、次のステートにおいて、その命令のオペランドコードが格納されている位置を指すアドレスAD+1となる。

【0035】したがって、命令レジスタ12には、図4（d）に示すように、前の命令サイクルの最終ステートにおいて命令コードが格納され、次のステートにおいてオペランドコードが格納される。一方、図4（c）に示すように、プログラムカウンタ11から出力される命令フェッチアドレスのうち、命令コードのアドレスADが命令フェッチアドレスレジスタ14に格納される。

【0036】続いて、命令デコーダ13は、命令レジスタ12に格納された命令コードをこの命令サイクルの最初のステートで解釈し、分岐命令であれば、制御信号を出力して、バッファ22、24、26をイネーブル状態にし、セクタ21がプログラムカウンタ11の出力を選択するように制御する。

【0037】これにより、命令コードの次に命令レジスタ12に格納されるオペランドコードが、分岐先のアドレスNとしてバッファ24を介してアドレスバス6に出力され、さらにバッファ26を経由してプログラムカウンタ11に格納される。こうして、プログラムカウンタ11から出力される命令フェッチアドレスが、図4

（b）に示すように、アドレスNとなる。そして、この命令フェッチアドレスは、セクタ21を介してマスクROM2に与えられ、バッファ22、アドレスバス6を介してEEPROM3に与えられる。

【0038】この命令フェッチアドレスがマスクROM2に割り当てられたアドレスであれば、ROM2の該当アドレスの命令語がインストラクションバス7に出力され、EEPROM3に割り当てられたアドレスであれば、ROM3の該当アドレスの命令語がインストラクションバス7に出力される。そして、インストラクションバス7に出力された命令語は、命令レジスタ12に格納される。こうして、分岐処理が行われる。

【0039】プログラムカウンタ11から出力される命令フェッチアドレスは、通常、命令フェッチと命令実行に伴って、初期設定値からインクリメントしながら更新されていくが、上記のように分岐命令がメモリから読み出されると、分岐先のアドレスに更新されて、プログラム実行のアドレス分岐が行われる。

【0040】以上のような分岐命令フェッチと分岐命令実行において、メモリから読み出された命令が保護領域への分岐命令であった場合には、その命令がどのメモリエリアから読み出されたものかを識別して、保護領域への分岐が許されているエリアから読み出された命令であれば、通常通り分岐を実行するが、保護領域への分岐が許されていないエリアから読み出された命令であれば、

分岐命令の実行を禁止する。次に、この動作について説明する。

【0041】まず、エリアテーブル15には、マスクROM2あるいはEEPROM3内の保護領域のアドレスが格納され、エリアテーブル16aには、保護領域への分岐が許されている分岐命令の命令フェッチアドレスが格納されている。これらの情報の設定の仕方は、実施の形態の1と同様でよい。

【0042】アクセス検出回路17aは、命令デコーダ13が分岐命令であると識別したとき、エリアテーブル15に保持されたアドレスとアドレスバス6に出力されたアドレス（オペランドコードから得られた分岐先のアドレス）とを比較して、保護領域への分岐命令かどうかを判定する。

【0043】つまり、アクセス検出回路17aは、エリアテーブル15に登録されたアドレス範囲中にアドレスバス6に出力されたアドレスと一致するものがあれば、保護領域への分岐命令と判断し、一致するものがなければ、保護領域への分岐命令ではないと判断する。

【0044】続いて、比較回路18aは、アクセス検出回路17aが保護領域への分岐命令であると判断したとき、命令フェッチアドレスレジスタ14に保持された命令フェッチアドレスとエリアテーブル16aに保持された命令フェッチアドレスとを比較して、保護領域への分岐が許されているエリアから読み出された命令かどうかを判定する。

【0045】つまり、比較回路18aは、エリアテーブル16aに登録された命令フェッチアドレス中に命令フェッチアドレスレジスタ14に保持された命令フェッチアドレスと一致するものがあれば、保護領域への分岐が許されているエリアから読み出された命令であると判断し、一致するものがなければ、保護領域への分岐が許されていないエリアから読み出された命令であると判断する。そして、比較回路18aは、保護領域への分岐が許されていないエリアから読み出された命令であると判断したときに、禁止信号を出力する。

【0046】コントロール回路20aは、比較回路18aから禁止信号が出力されると、CPU1aの外部からリセット信号が入力されたときと同様のCPUリセットが実施される内部リセット信号を図5（f）のように出力し、CPUリセットをかける。同時に、この内部リセット信号はCPU1aの周辺回路にも出力され、CPU周辺の回路についても同様にリセットされる。

【0047】内部リセット信号が出力されると、プログラムカウンタ11がゼロクリアされるために、命令フェッチアドレスは、図5（b）に示すように、「0000」となる。これにより、分岐命令のステータス後はリセットベクタ処理ルーチンが実行される。

【0048】サブルーチン（サブプログラム）がROM2あるいはROM3上に書き込まれていた場合、サブ

ーチンを読み出そうとする第3者は、サブルーチンをコールするような命令プログラムをメモリに書き込むことが考えられる。通常、このようなサブルーチンが書き込まれているアドレスは、第3者には知りえないものであるが、周辺装置の動きや、そのときのデータバス5、アドレスバス6上のデータを外部からモニタすることにより、予測することは可能である。この場合、サブルーチンに大量の解析用データを順次与え、得られた膨大な結果から処理結果を解析することにより、サブルーチンで行っている処理内容が解説されるおそれがある。

【0049】本実施の形態によれば、エリアテーブル15、16aにアドレス情報を予め設定しておくことにより、保護領域へ分岐しない命令、あるいは保護領域へ分岐する命令であっても、保護領域への分岐が許されているエリアから読み出された命令であれば、正常に実行され、一方、保護領域への分岐が許されていないエリアから読み出された命令であれば、不正な命令プログラムと判断されて、処理がリセットされる。

【0050】したがって、第3者がEEPROM3上に不正な命令プログラムを書き込んだとしても、ROM2あるいはROM3上の保護領域のサブルーチンをコールすることはできず、このサブルーチンに解析用データを与えることはできない。

【0051】なお、本実施の形態では、コントロール回路20aを禁止手段としているが、比較回路18aから出力される禁止信号を命令デコード13に与えることにより、命令デコード13を禁止手段としてもよい。命令デコード13は、分岐命令をフェッチしたとき、プログラムカウンタ11の値を分岐先のアドレスに更新する制御を行うが、比較回路18aから禁止信号が入力されると、アドレスを更新するための制御信号にマスクをかける。

【0052】よって、禁止信号が出力されると、プログラムカウンタ11から出力される命令フェッチアドレスは、分岐先のアドレスに更新されることなく、通常通りに+1インクリメントされるので、実質的にはNOP (NO Operation) 命令が実行されたときと同じとなる。こうして、上記と同様の効果を得ることができる。

【0053】また、禁止信号が出力されたとき、コントロール回路20aが、CPU1aの外部からインタラプト信号が入力されたときと同様の割り込み処理をかけてもよい。この場合は、ノンマスク割り込みが強制的に起動し、割り込み処理ルーチン内で何らかの処理（例えば、不正なアクセスである旨を表示装置上に表示するなど）が行われることになる。

【0054】また、複数の命令を決められた命令フェッチアドレス順に実行した後に分岐命令を実行する以外は、分岐命令の実行を禁止するようにすれば、保護機能をより高めることができる。

【0055】これは、複数の命令コードの命令フェッチ

アドレスを命令フェッチアドレスレジスタ14に格納できるようにして、エリアテーブル16aに保護領域への分岐が許されている分岐命令の命令フェッチアドレスだけでなく、この分岐命令の前に実行される複数の命令の命令フェッチアドレスを設定し、比較回路18aでレジスタ14とテーブル16aの内容を比較させればよい。

【0056】なお、実施の形態の1、2では、メモリの構成をマスクROM2、EEPROM3、RAM4からなるものとしているが、これに限るものではない。また、バスの構成をデータバス5、アドレスバス6、インストラクションバス7の3本としているが、インストラクションバスがないものでも構わない。この場合は、データバス上にデータと命令が時分割に存在することになる。また、RAM4に保護領域があってもよく、RAM4から命令をフェッチしてもよい。

【0057】

【発明の効果】本発明によれば、請求項1に記載のように、アクセス検出手段によって保護領域へのアクセス命令かどうかを判定し、保護領域へのアクセス命令が検出されたとき、保護領域へのアクセスが許されている格納位置から読み出された命令かどうかを比較手段によって判断し、保護領域へのアクセスが許されていない格納位置から読み出された命令と判断したときに、不正なアクセスと見なして禁止信号を出力し、禁止手段によってメモリアccessを禁止することにより、保護領域への不正なアクセスを禁止することができるので、保護領域のデータを保護することができ、高い保護機能を実現することができる。よって、メモリ間の転送命令のみならずメモリアccessに係わる全ての命令に対して不正なアクセスかどうかを判定するので、保護領域内のデータをメモリに直接読み出さずに保護領域内のデータに何らかの演算を行ってデータ内容を間接的に知ることでもできなくなる。

【0058】また、請求項2に記載のように、アクセス検出手段によって保護領域への分岐命令かどうかを判定し、保護領域への分岐命令が検出されたとき、保護領域への分岐が許されている格納位置から読み出された命令かどうかを比較手段によって判断して、保護領域への分岐が許されていない格納位置から読み出された命令と判断したときに、不正な命令と見なして禁止信号を出力し、禁止手段によって分岐命令の実行を禁止することにより、保護領域への不正な分岐を禁止することができるので、保護領域のサブプログラムを保護することができる。これにより、外部からの不正なアクセスにより、不要に保護領域内の命令プログラムを実行させることを禁止し、第3者による命令プログラム解説等の不正なアクセスを妨げることができる。

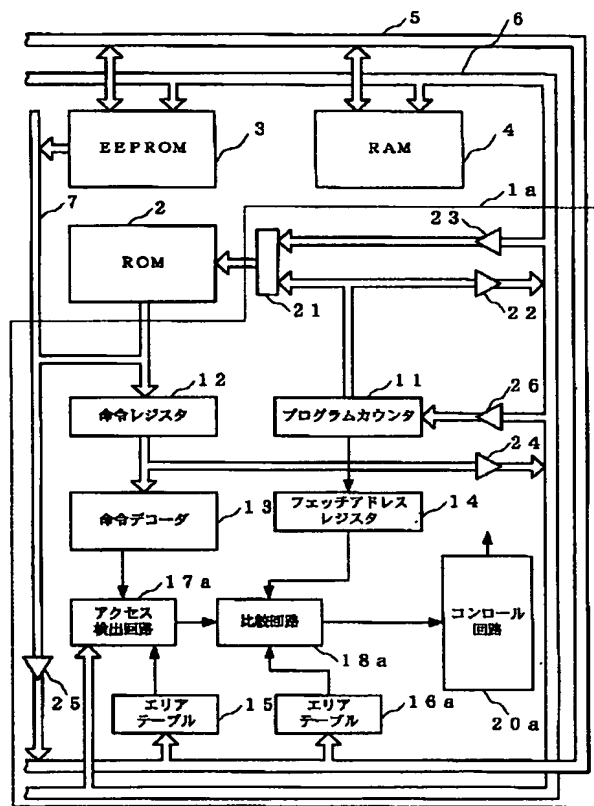
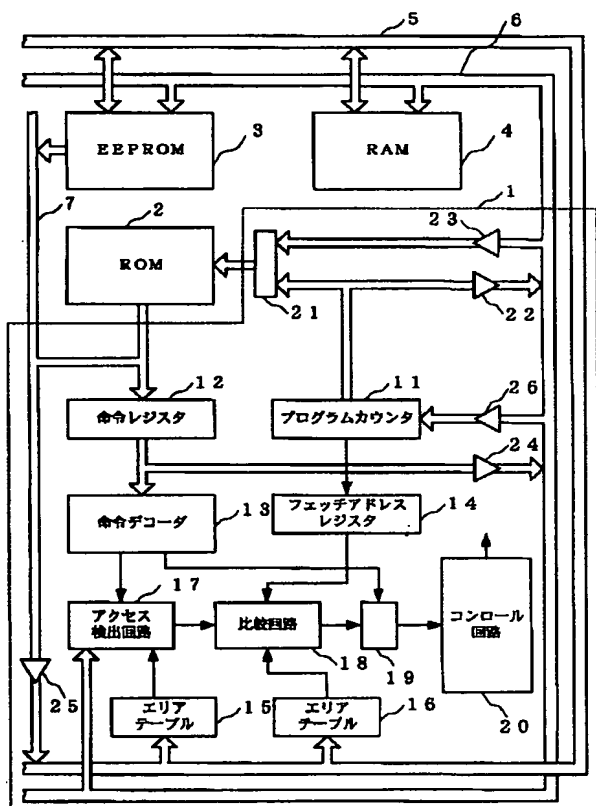
【図面の簡単な説明】

【図1】 本発明の第1の実施の形態を示すメモリアccess制御回路のブロック図である。

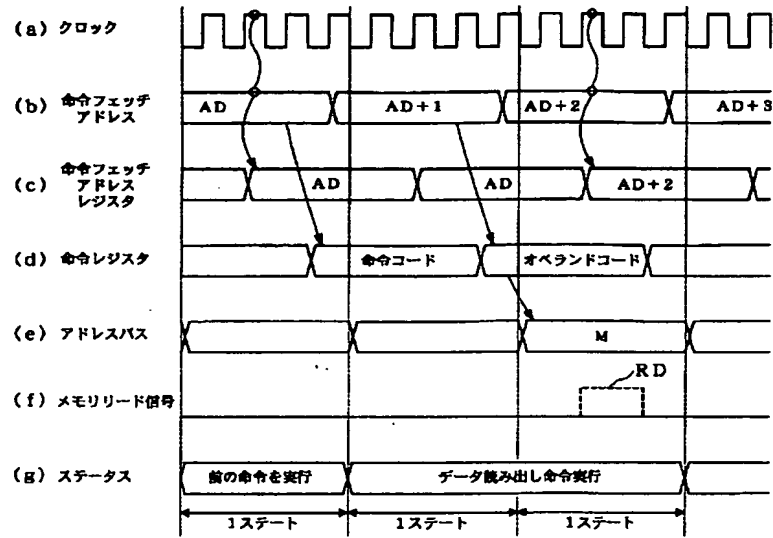
【図6】 従来のメモリアクセス制御回路のブロック図である。

1、1 a…CPU、2…マスクROM、3…EEPROM、4…RAM、5…データベース、6…アドレスバス、7…インストラクションバス、11…プログラムカウンタ、12…命令レジスタ、13…命令デコーダ、14…命令フェッチアドレスレジスタ、15、16、16 a…エリアテーブル、17、17 a…アクセス検出回路、18、18 a…比較回路、19…ゲート回路、20、20 a…コントロール回路。

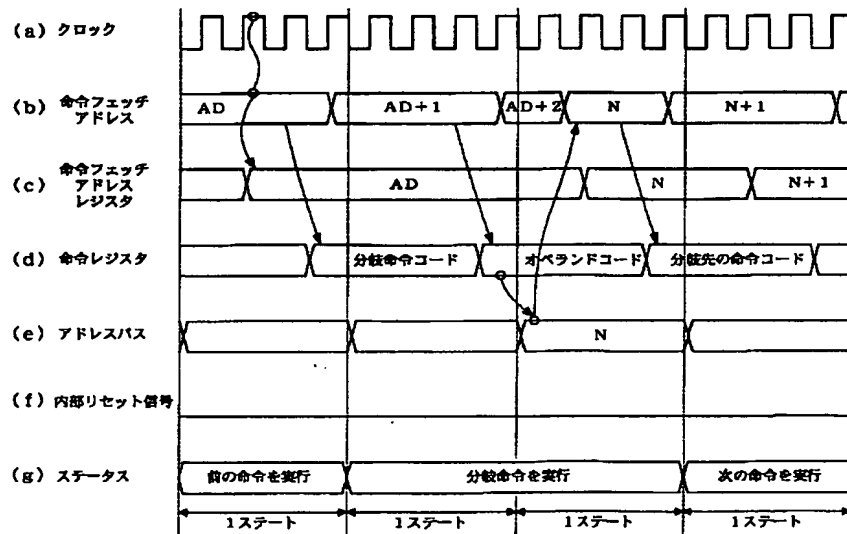
【图 3】



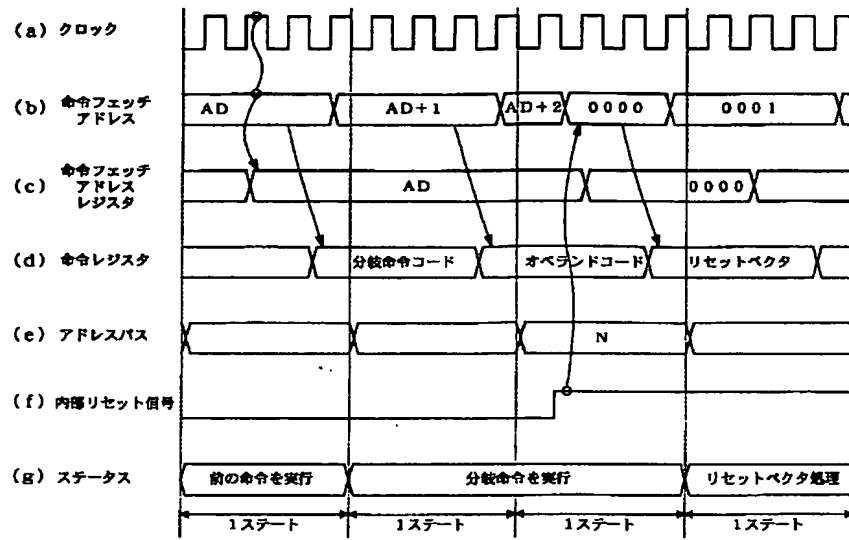
【図2】



【図4】



【図 5】



【図 6】

